THOMAS KRENN®

IT-Sicherheit Rückblick 2022

Webinar am 24.01.2023

Christoph Mitasch, Thomas-Krenn.AG

THOMAS KRENN®

Christoph Mitasch

- seit 2005 bei der Thomas-Krenn.AG, Niederlassung Österreich
- Diplomstudium Computer- und Mediensicherheit
- Erfahrung in Web Operations, Linux und HA
- Cyber-Security-Practitioner (v1)
- IT-Sicherheitsbeauftragter

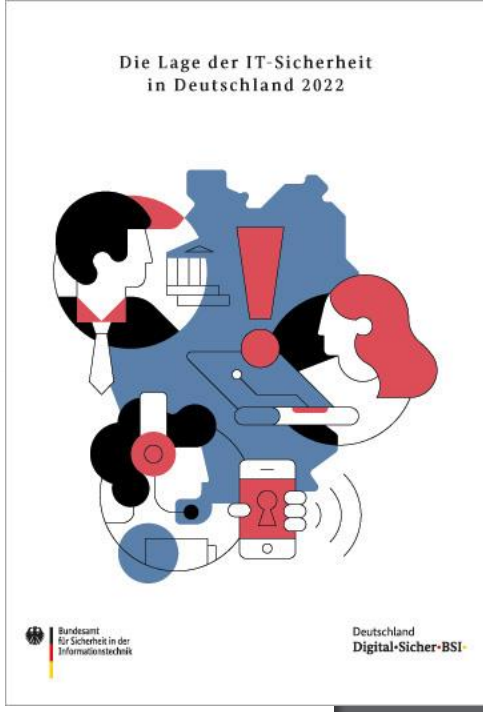
Agenda

Lagebericht BSI 2022

MFA Fatigue

Update Log4j & MS Exchange

Lagebericht BSI 2022



- „Insgesamt spitzte sich im Berichtszeitraum die bereits zuvor angespannte Lage weiter zu.“
- „Die Bedrohung im Cyber-Raum ist damit so hoch wie nie.“
- „Ransomware blieb die Hauptbedrohung, besonders für Unternehmen.“
- „Hinzu kamen verschiedene Bedrohungen im Zusammenhang mit dem russischen Angriffskrieg auf die Ukraine.“

https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft

Identitätsdiebstahl
Sextortion
Fake-Shops im Internet

Wirtschaft

Ransomware
Schwachstellen, offene oder falsch konfigurierte Online-Server
IT-Supply-Chain: Abhängigkeiten und Sicherheit

Staat und Verwaltung

Ransomware
APT
Schwachstellen, offene oder falsch konfigurierte Online-Server

Erster digitaler Katastrophenfall in Deutschland

207 Tage Katastrophenfall

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

Die Anzahl der Schadprogramme steigt stetig.

Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund

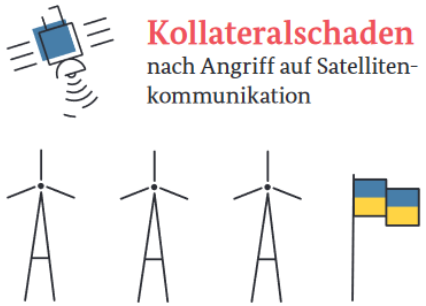
116,6 Millionen zugenommen.

Hacktivismus im Kontext des russischen Krieges:

Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.

Kollateralschaden

nach Angriff auf Satellitenkommunikation



20.174

Schwachstellen in Software-Produkten (13 % davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10 %** gegenüber dem Vorjahr.

15 Millionen Meldungen zu Schadprogramm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.

34.000

Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.

78.000

neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

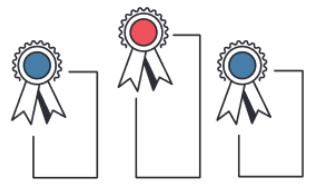
69%

aller Spam-Mails im Berichtszeitraum waren Cyber-Angriffe wie z. B. Phishing-Mails und Mail-Erpressung.

90%

des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d. h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.

BSI ist weltweit der führende Dienstleister im Bereich Common-Criteria-Zertifikate.



5.100 2021
4.400 2020

Zehn Jahre Allianz für Cyber-Sicherheit:
2022 sind wir bereits
6.220 Teilnehmer.

Deutschland
Digital•Sicher•BSI•

Bundeslagebericht BKA 2021

Cybercrime gemeinsam bekämpfen

Strafverfolgung und Unternehmen kennen einander, kooperieren aber nur bedingt - Straftäter hingegen kennen einander nicht, kooperieren aber vertrauensvoll auch über Ländergrenzen hinweg.

Cybercrimefighting-as-a-Service

Cybercrime-as-a-Service fordert entsprechende Entwicklungen auch auf Seiten der Strafverfolgungsbehörden.

Aufklärungsquote 2021 sank auf unter 30%

Ransomware

LÖSEGELD / RANSOM

Coveware beziffert die durchschnittliche Ransom im Jahr 2021 auf 204.695 US-Dollar. 2020 betrug die geforderte Ransom im Durchschnitt "nur" 169.446 US-Dollar.

Tendenziell steigen die pro Erpressungsfall geforderten Summen an.

SCHÄDEN

Ransomware verursachte laut Studie "Wirtschaftsschutz 2021" des Bitkom e.V. einen jährlichen Schaden von ca. 24,3 Mrd. Euro. 2019 betrug diese Zahl noch 5,3 Mrd. Euro.

Das Schadenspotenzial von Ransomware nimmt rasant zu.

KRIMINELLE EINNAHMEN

Laut Chainalysis haben Ransomware-Gruppierungen im Jahr 2021 602 Millionen US-Dollar in Form von Kryptowährungen erpressen können.

Modi Operandi

Double Extortion:
Der Standard-Modus-Operandi (Datenverschlüsselung und -veröffentlichung).

Triple Extortion:
Zusätzlich zur Datenverschlüsselung und -veröffentlichung erfolgen DDoS-Attacken beim Opfer.

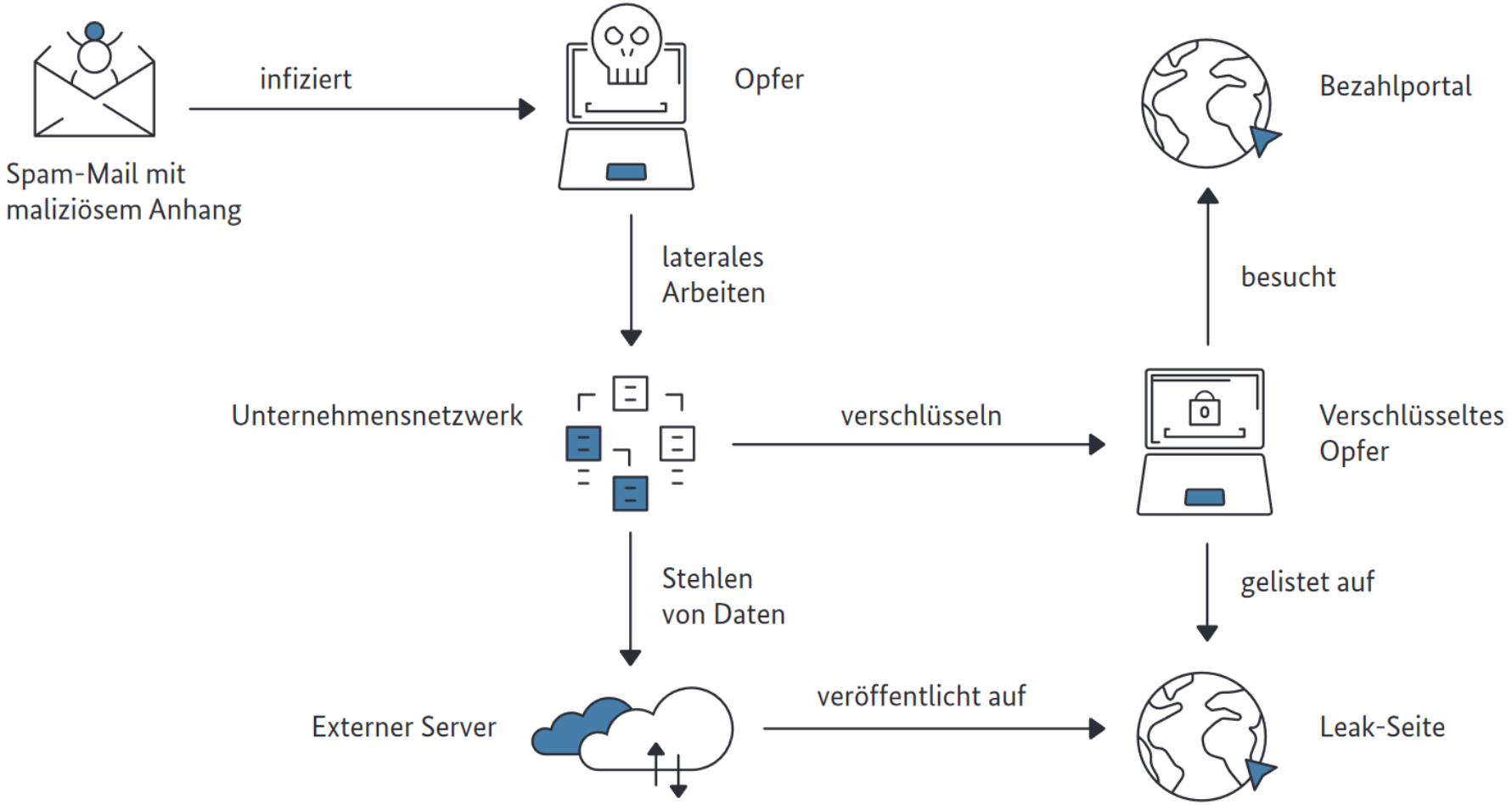
Second-Stage-Extortion:
Auch Kunden der eigentlichen Opfer werden damit erpresst, dass Ihre Daten veröffentlicht werden, sollte keine Zahlung erfolgen.

https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.pdf?__blob=publicationFile&v=6

Ablauf Ransomware

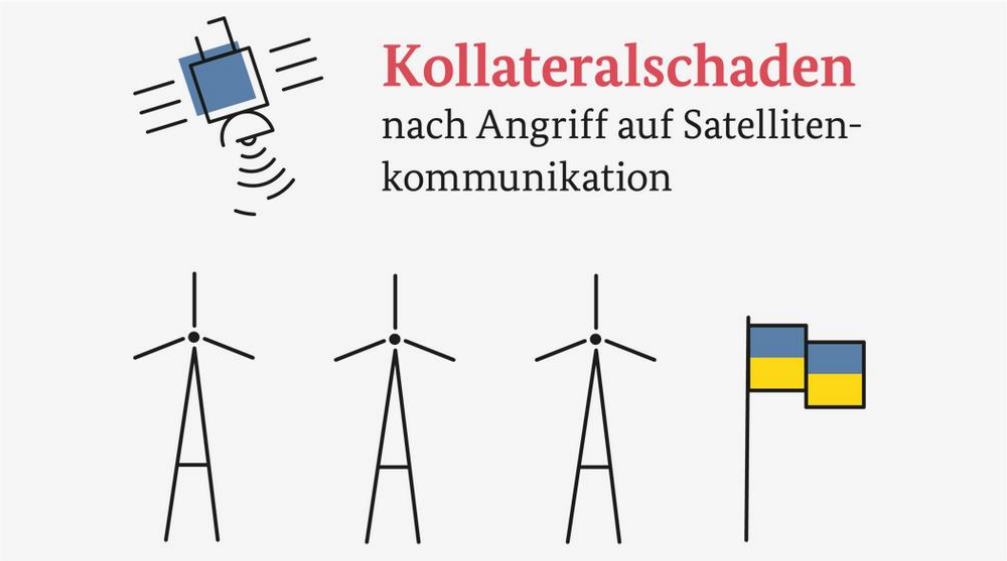
Beispielhafter Angriffsablauf

Abbildung 3:
Beispielhafter Ablauf eines Ransomware-Angriffs mit Lösegeld- und Schweigegelderpressung (schematische Darstellung)
Quelle: BSI



Auswirkungen durch Krieg

- DOS auf Modems der Windkraftanalgen
  - exakt mit Kriegsbeginn am 24. Februar 2022
  - Fernwartung für 5.800 Windenergieanlagen betroffen
  - Ursprung Cyberangriff in der Ukraine
- Deutscher Mineralölhändler
  - März 2022, russischer Mutterkonzern
  - Angriff durch Gruppe Anonymous Deutschland
  - Systeme kompromittiert und heruntergefahren
  - Für Notbetrieb erforderliche Dienstleister verweigerten Zusammenarbeit wegen Sanktionen



Quelle BSI

- Wiper auf Ukrainische Banken im Einsatz
- Industroyer2 im April 2022 in ukrainischen Umspannwerken -> konnte noch deaktiviert werden
- Störungen IT-Lieferketten, Hardware schlecht verfügbar
  -> Resilienz gegen Cyber-Angriffe weiter erhöhen

https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Charity Scam

Von: Für Menschen mit Herz <mail@world-of-shopping-mail.de>
Gesendet: 27. Februar 2022 14:37
An: [redacted]
Betreff: +++ Ukraine: Hilfe dringend benötigt +++

Sollte der Newsletter nicht richtig dargestellt werden, klicken Sie bitte hier

Malteser International
Order of Malta Worldwide Relief

Malteser
...weil Nähe zählt.

Liebe Leserin, lieber Leser,

wir alle hatten die Hoffnung, dass die Ukraine und Russland ihren Konflikt ohne weitere kriegerische Handlungen lösen. Heute kamen dann die unfassbaren Nachrichten: Russland hat die Ukraine angegriffen.

Kaspersky

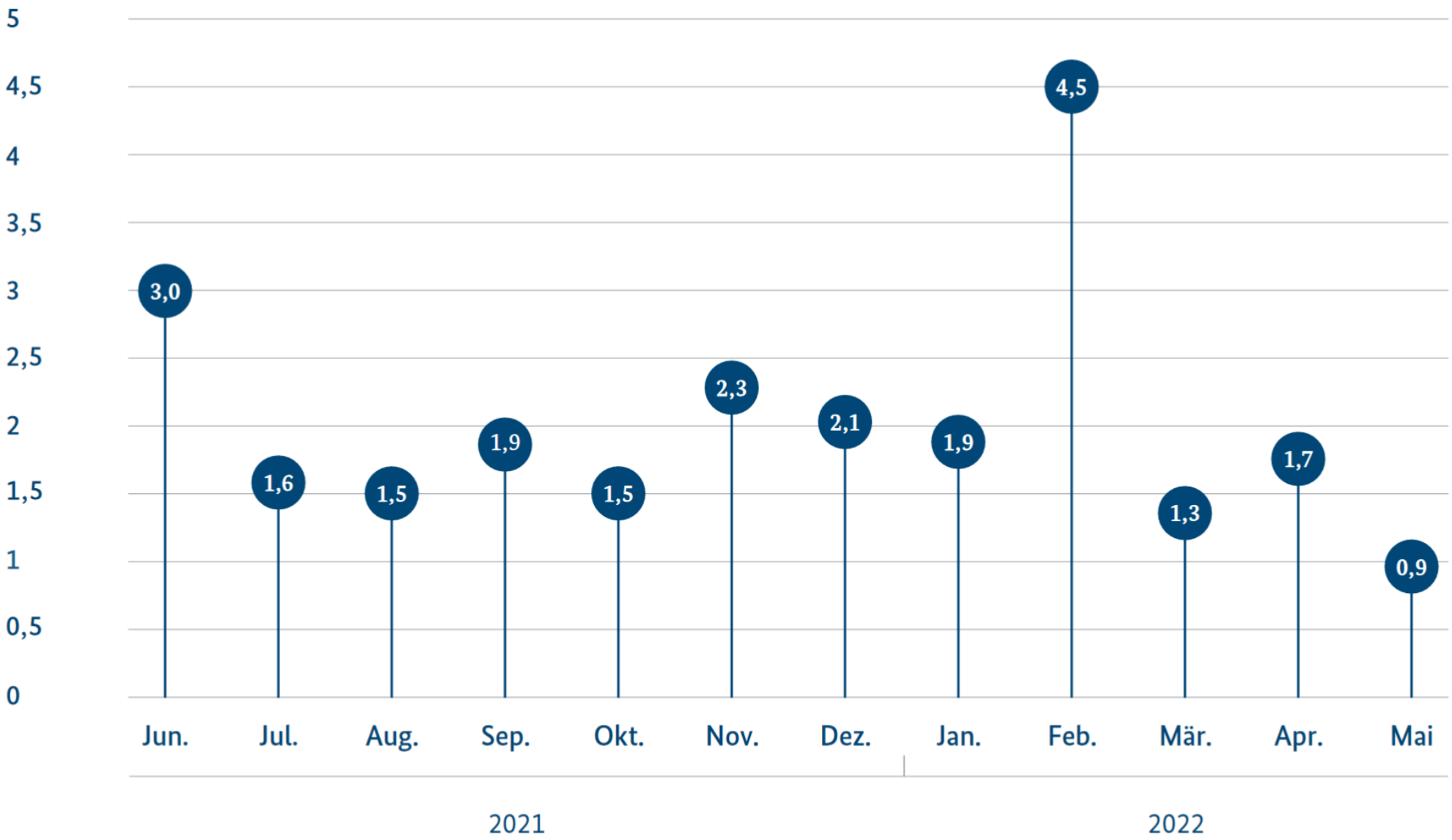
- BSI am 15. März 2022 vor Kaspersky-Virensoftware gewarnt
- Warnung nach §7 BSI-Gesetz
  - teilweise kritisiert als politisch motiviert
  - Bestätigung durch Oberverwaltungsgericht im Jänner 2023
- auch Verbraucher sollen Umsteigen
- Devise „Ablösen statt Abschalten“

https://www.publicdomainpictures.net/de/view-image.php?image=261650&picture=antivirus

Spam-Ratio in der Wirtschaft in Deutschland

Anzahl Spam-Mail je legitime, erwünschte E-Mail

Abbildung 11:
Spam-Ratio in der Wirtschaft in Deutschland
Quelle: E-Mail-Verkehrsstatistik



OpenAI, ChatGPT

OpenAI

- KI als Chance und Risiko
- Phishing-Mails werden durch KI gefährlicher und interaktiver
- Malware kann generiert werden
- Social Bots
- KI-Systeme selbst als Ziel
- KI sollte zukünftig auch zur Abwehr eingesetzt werden
- Microsoft investiert viel in OpenAI -> Azure OpenAI Service

„Das größte Fragezeichen wird sein, wie wir als Menschen in Zukunft unterscheiden können, ob eine Information von einem Menschen oder von einer KI erstellt wurde. Welchen Informationen sollten wir vertrauen? Bis jetzt haben wir als Gesellschaft noch kein Modell entwickelt, um Missbrauch zu verhindern, aber das müssen wir vielleicht eher früher als später tun."

Markus Grau, Pure Storage

https://www.is-its.org/it-security-blog/kuenstliche-intelligenz-und-it-sicherheit-chance-oder-bedrohung
https://www.it-business.de/chatgpt-mehr-fluch-als-segen-das-sagt-die-security-branche-a-d221f9f8d26794497b1926cf6ee9284ec3/

Agenda

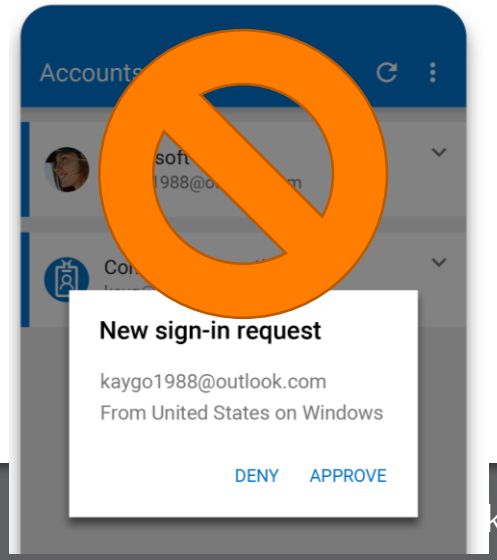
Lagebericht BSI 2022

MFA Fatigue

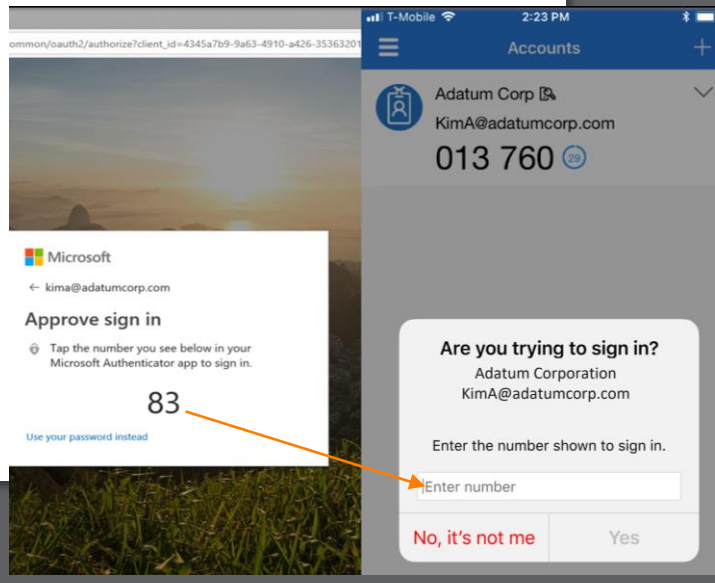
Update Log4j & MS Exchange

MFA Fatigue

- Vorfall bei Fahrdienst Uber
- Computer von Mitarbeiter kompromittiert, Login-Daten für Uber aus Darknet
- Mitarbeiter wurde so lange mit MFA-Anfragen genervt, bis er bestätigt hat
  -> MFA alleine ist oft zu wenig, kommt auf sichere Implementierung an
- BSI Bewertungstabellen zu 2FA
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/2FA/it-sicherheit.pdf?__blob=publicationFile&v=3
- PUSH mit DENY/APPROVE ist anfällig



Numbers Matching ist wesentlich sicherer



https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=de&gl=US
https://learn.microsoft.com/de-de/azure/active-directory/authentication/how-to-mfa-number-match

Agenda

Lagebericht BSI 2022

MFA Fatigue

Update Log4j & MS Exchange

Log4j

- Log4j Sicherheitslücke 1 Jahr alt
  - wird weiterhin gezielt für Angriffe genutzt
  - per 1.10.2022 waren 72% der Firmen anfällig
    -> fast 1/3 davon ist wieder anfällig geworden (laut Tenable)
  - schwierig es komplett und längerfristig aus großer IT rauszubekommen
    häufig im Bundle dabei
  - kann auch interne Systeme betreffen, die nicht im Internet
    erreichbar sind aber Logs von Systemen im Internet verarbeiten

Über Log4j: US-Behörde vom Iran attackiert, Cryptominer installiert

Die CISA hat einen Angriff auf eine ungenannte US-Regierungsinstitution registriert, bei dem die Log4j-Lücke ausgenutzt wurde. Die bleibt ein Problem.

Lesezeit: 2 Min. In Pocket speichern 12

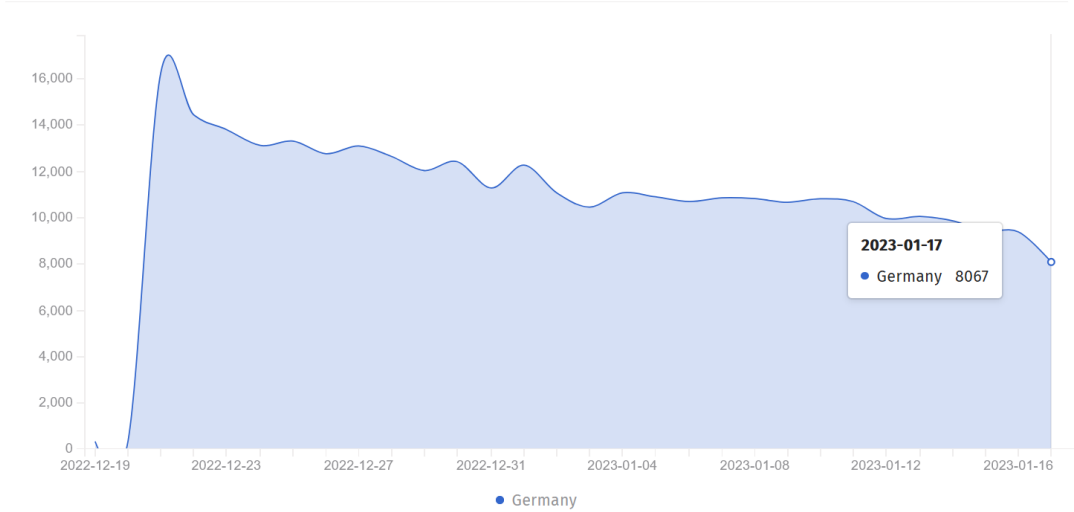
(Bild: JLStock/Shutterstock.com)

17.11.2022 17:22 Uhr

https://www.heise.de/news/Ueber-Log4j-US-Behoerde-vom-Iran-attackiert-Cryptominer-installiert-7343471.html
https://www.tenable.com/press-releases/tenable-research-finds-72-of-organizations-remain-vulnerable-to-nightmare-log4j
https://riskledger.com/blog/emerging-threats-in-the-supply-chain

MS Exchange

Results



https://dashboard.shadowserver.org/statistics/combined/time-series/?date_range=30&source=scan%2Bscan6&tag=exchange&geo=DE&style=stacked

- ProxyNotShell (CVE-2022-41040, CVE-2022-41082)
  - Beliebige Remote Code Execution für authentifzierte Angreifer
  - Exchange Server 2013/2016/2019
  - Mitigation Service hat geholfen, wurde aber immer wieder umgangen
  - Update am 9.11.2022, über 1 Monat gedauert, davor nur Workarounds
  - Mitte Jänner noch immer > 8000 betroffene Server in Deutschland
- Altbekannte Empfehlungen noch immer aktuell
  - Cert.at:

Ein On-Prem Exchange-Server ist nur dann ein sicherer oder zumindest halbwegs sicherer Exchange-Server, wenn seine Webinterfaces (Outlook Web Access, Exchange Web Services, etc) ausschließlich über private, gesicherte Verbindungen (zum Beispiel VPN) erreichbar sind.

Verfasst von: Erik Huemer

Generell empfiehlt CERT.at, sämtliche Software aktuell zu halten und dabei insbesondere auf automatische Updates zu setzen. Regelmäßige Neustarts stellen sicher, dass diese auch zeitnah aktiviert werden.

Verfasst von: Michael Schlagenhaufer

Ausblick und Empfehlungen

- „85% aller Angriffe starten beim Faktor Mensch“ -> Awareness Training
- Ransomware
  -> Backup, offline, Restore-Test
  -> Monitoring des Datentransfers
  -> Notfallkonzepte + Übung
- Updates
  -> Zero Day Tuesday und Hack Wednesday
  -> automatische Updates + Monitoring
  -> Cert.at Daily - https://cert.at/de/services/mailinglisten/
- Endpoint Detection und Response
- Allianz für Cybersicherheit Podcast „CYBERSNACS“
- Heise Security Pro

https://sosafe-awareness.com/de/ressourcen/reports/human-risk-review/

THOMAS KRENN®

Vielen Dank für Ihre Aufmerksamkeit!